UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/861,989	05/22/1997	KELLY EUGENE DILLARD	60323	2874

7590 11/03/2004

JEANNE C. SUCHODOLSKI
ALLIED SIGNAL INC. - LAW DEPARTMENT
101 COLUMBIA ROAD
P.O. BOX 2245
MORRISTOWN, NJ 07962

EXAMINER	
CARLSON, JEFFREY D	
ART UNIT	PAPER NUMBER
3622	

DATE MAILED: 11/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 08/861,989
Filing Date: May 22, 1997
Appellant(s): DILLARD ET AL.

Monique Perdok Shonka
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/13/04.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The rejection of claims 25-30 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

WO 90/13865	HORNBUCKLE	11-1990
5,951,620	AHRENS et al	9-1999

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 25-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Behr et al (US6107944) in view of Hornbuckle (WO 90/13865) and Ahrens et al (US5951620). Behr et al teaches a method for providing software updates to mobile/remote GPS units. The remote GPS unit requests data (via user interface display/keyboard 24, 28, 30, 46, 60 - fig 1) from a base unit and the most recent maps/navigation data are transmitted to the remote unit. "The amount of information available at the remote unit can be increased by providing the remote unit with information from the base unit which is not adequately covered by any databases on-board the remote unit" [see abstract]. Behr et al, like applicant, recognizes the same limitations of prior art systems in which GPS/navigation units that require updates of more recent navigation/map data have to rely on distribution of floppy disk or CDs col 2 lines 4-24]. The remote units request data from the base unit which responds with the requested data. Behr et al's methods include a database of maps located at the remote GPS unit [col 21 lines 33-36]; updates to the maps and programs can be communicated from the base unit to the remote unit to provide most recent versions [col 22 lines 9-12]. The communication protocol includes features for CRC error checking, compression, as well as inclusion of unitID and subscriberID information for billing purposes [col 6 lines 40-46, col 11 lines 59-65, col 12 lines 57-62, col 14 lines 1-3, 10-14]. Regarding the

"payment authorization information", as broadly interpreted this merely requires any type of information that is associated with authorization of payment. It is noted that no steps/structure is required by the claims to authorize or process any particular payment; only information that has a mere *association* to payment authorization need be provided. As such, requests for updated navigation information are taken to include payment authorization information and/or permission for charging payments in that they at least identify a subscriber and are associated with billing function(s). Behr et al does not teach encryption however. Hornbuckle teaches distribution of software code using encryption techniques so that the software can only be used by the intended recipient hardware [pg 21 lines 15-19]. The functionality of the software transmitted by Hornbuckle's methods is not the focus of the rejection, but rather the motivation for securing the transmitted software. It would have been obvious to one of ordinary skill at the time of the invention to have provided such encryption techniques with the GPS remote hardware devices of Behr et al so that the data transmissions over Behr et al's non-secure facilities (telephone system, RF, etc) were secured and that Behr et al's desire for sending software only to paying customers was accomplished in a way that prevents unauthorized, non-paying customers from accessing such data. Hornbuckle teaches encryption/decryption using an encryption key derived from and unique to the individual target deviceID in which the requested software is to be used [pg 20 lines 20-23]. Hornbuckle teaches downloading a decrypting module/program along with the encrypted requested software. The decrypting module decrypts the requested software and loads it into the internal memory of the targeted device [pg 19 lines 21-31]. The

downloaded software package will only run on the particular target device having an encryption key corresponding to the encryption key employed by the host when the software was encrypted [pg 21 lines 15-19]. This encryption and decryption algorithm which uses the same key is an example of symmetric, or single-key encryption. Symmetric encryption requires both parties to possess the same key. Official Notice is taken that distribution of the needed key can be provided by either party. Hornbuckle appears to provide an example where the host sends the key to the client. It would have been obvious to one of ordinary skill at the time of the invention to have alternatively provided the host with a copy of the client key (unique to the user hardware) as part of the initial request, so that both parties have copies of the same key, consistent with the symmetric encryption approach. It is a matter of system design choice to choose who transmits a copy of the key, so long as both parties use the same key. The requested software will have the decrypting program/module appended and the original software will be replaced with the encrypted software [pg 21 lines 27-30]. This appending is taken as providing the decrypting program in the footer of the transmission. It would have been obvious to one of ordinary skill at the time of the invention to have relied on and transmitted the unique GPS unitID taught by Behr et al to the base unit for encryption purposes so that the encrypted software can only be decrypted and used by the authorized device possessing the same GPS unitID key; likewise, it would have been obvious to one of ordinary skill at the time of the invention to have verified the presence of the proper unique key in the transmission footer so that decryption can only occur properly for the intended recipient device. Ahrens et al

teaches a GPS system whereby users may pay for subscriptions entitling them to downloaded GPS map updates [abstract, col 19 lines 63+]. The user's GPS device is provided media *within* the GPS unit which stores the unitID; this unitID is used for security purposes to ensure updates can only be made to the appropriate device. It would have been obvious to one of ordinary skill at the time of the invention to have provided such hardware identification with that of Behr et al and Hornbuckle as an example of how to carry out the required hardware identification taught by Behr et al and Hornbuckle. Ahrens et al also points out that his transmitted GPS updating methods can also be used for other types of software, including PC software and computer game software. This strengthens examiner's argument that one of ordinary skill would be motivated to use Hornbuckle's encryption techniques when transmitting software; secure transmission of software is critical, regardless of the software's ultimate functionality.

Regarding the "navigation data" language, the types of data in the "geographical databases" (described as route guidance, streets, airports, restaurants, points of interest, etc [col 1 lines 37-62]) of Behr et al can be taken to be navigation data - one could navigate by relying on the data in Behr et al's "geographical databases"; Navigation can be accomplished by using maps of highways, rivers, buildings, etc.

Regarding claims 26, 27, it would have been obvious to one of ordinary skill at the time of the invention to have employed any well known encryption techniques, including CRC encryption using the unique unitID as a seed. Any encryption technique

could have been used to secure the transmission and such selection of techniques is not critical to the invention.

(11) Response to Argument

Applicant argues that it is not possible in Hornbuckle to send the key to the host from the client. This argument is not understood by the examiner, however examiner has supplied evidence supporting Official Notice. Further, the rejection proposes the obvious modification of sending Behr et al's unitID as the encryption key to the software supplier host.

Applicant argues that the references do not provide "payment authorization information." As stated above, "payment authorization information" as broadly interpreted merely requires any type of information that is associated with authorization of payment. As such, requests for updated navigation information are taken to inherently include payment authorization information and/or permission for charging payments in that they at least identify a subscriber and are associated with billing functions. It is further noted that no steps/structure is required by the claims to authorize or process any particular payment; only information that has a mere *association* to payment authorization need be provided. Applicant's argument that the instant specification (pg 8 lines 3-10) defines the language in question is not convincing. There is no explicit definition of "payment authorization information," but rather a statement that in fact requiring payments is optional and general disclosure that various electronic payment systems can be used to purchase updates if desired. The claim

language is therefore broadly but reasonably interpreted using the plain and ordinary meaning of the language.

Applicant argues that there is no suggestion to combine Behr et al and Hornbuckle because there is no need or desire in Behr et al for encryption/security. Applicant admits [spec pg 2] that GPS software providers typically provide software updates via mailed floppy disks rather than via the Internet to prevent easily unauthorized duplication of such Internet-distributed software. Applicant notes problems with floppy disk distributions. Applicant also admits the known problem of an authorized update being easily applied to an unauthorized device. Behr et al also notes the problems with floppy disk distribution of software/map updates [col 2 lines 4-24]. Behr et al teaches that users are subscribers and are billed for services. One of ordinary skill would be motivated to protect against such known software pirating in the case of Behr et al's subscribing customers purchasing software services. Further, Hornbuckle also supplies reasoning to secure/encrypt software updates so that only paying, authorized users can use them.

Applicant states that because Behr et al's updates are for a single, user-specified route, that it is of no value to others. Examiner disagrees with such an opinion. Beyond the motivation to secure the purchased data for use only by the authorized/paying user, the GPS user may desire privacy for his selected route details/updates.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jeffrey D. Carlson
Primary Examiner
Art Unit 3622

jdc
October 29, 2004

Conferees
Eric Stamber
James Myhre

JEANNE C. SUCHODOLSKI
ALLIED SIGNAL INC. - LAW DEPARTMENT
101 COLUMBIA ROAD
P.O. BOX 2245
MORRISTOWN, NJ 07962